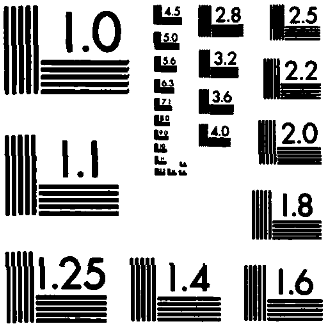
AD-A122 287 ROBUST AUTHENTICATION FOR THE NATIONAL SEISMIC SYSTEM 1/1
(U) INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA
SCIENCE AND TECHNOLOGY DIV J T BEARDWOOD JAN 82
UNCLASSIFIED IDA-P-1625 IDA/HQ-81-24010 MDA903-79-C-0202 F/G 8/11 NL

END
FILMED
DTIC



MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

AD-E500 552

Copy 26 of 45 copies

AD A122287

IDA PAPER P-1625

ROBUST AUTHENTICATION FOR THE NATIONAL SEISMIC SYSTEM

Joseph T. Beardwood

DTIC
ELECTE
DEC 10 1982
H

January 1982

Prepared for

Defense Advanced Research Projects Agency

DISTRIBUTION STATEMENT A
Approved for public release;
Distribution Unlimited

INSTITUTE FOR DEFENSE ANALYSES
SCIENCE AND TECHNOLOGY DIVISION

DTIC FILE COPY

82 12 01 041

IDA Log No. HQ 81-24010

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A122 287	3. RECIPIENT'S CATALOG NUMBER

4. TITLE (*and Subtitle*) Robust Authentication for the National Seismic System	5. TYPE OF REPORT & PERIOD COVERED FINAL Jan. 1 - Nov. 30, 1981
	6. PERFORMING ORG. REPORT NUMBER IDA PAPER P-1625
7. AUTHOR(s) Joseph T. Beardwood	8. CONTRACT OR GRANT NUMBER(s) MDA 903 79 C 0202
9. PERFORMING ORGANIZATION NAME AND ADDRESS INSTITUTE FOR DEFENSE ANALYSES 1801 N. Beauregard Street Alexandria, Virginia 22311	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS DARPA Assignment A-64
11. CONTROLLING OFFICE NAME AND ADDRESS DEFENSE ADVANCED RESEARCH PROJECTS AGENCY 1400 Wilson Boulevard Arlington, Virginia 22209	12. REPORT DATE January 1982
	13. NUMBER OF PAGES 68
14. MONITORING AGENCY NAME & ADDRESS(*if different from Controlling Office*)	15. SECURITY CLASS. (*of this report*) UNCLASSIFIED
	15a. DECLASSIFICATION/DOWNGRADING SCHEDULE --

16. DISTRIBUTION STATEMENT (*of this Report*)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (*of the abstract entered in Block 20, if different from Report*)

None

18. SUPPLEMENTARY NOTES

N/A

19. KEY WORDS (*Continue on reverse side if necessary and identify by block number*)

data compression, seismology, satellite, communication, authentication, cryptology, error correction, coding, redundancy, recording, National Seismic System, Seismic Control and Recording Station, Comprehensive Test Ban Treaty

20. ABSTRACT (*Continue on reverse side if necessary and identify by block number*)

During recent (1977-1980) trilateral negotiations between the U.S., the USSR, and the U.K. leading toward a Comprehensive Nuclear Test Ban Treaty, it was agreed that in order to monitor compliance with the treaty when it entered into force, unmanned, tamperproof seismic observatories would be installed on the territories of the three parties.

20. (Continued)

The seismic waveforms from each observatory are digitized and combined with other digital information concerning the status of the observatory. Each one second of the digital information is processed by a cryptologic algorithm whose output is appended to the data to permit authentication of the data (to prevent substitution or alteration), and the total digital signals transmitted, via satellite links, to the U.S., USSR, and U.K. for processing and analysis. Transmission errors with a prototype system resulted in an unacceptably high rate of authentication failures.

Nine options were examined to lower the rate of authentication failures. These included various combinations of bandwidth reduction, redundant paths, forward error correction coding, and post-reception processing. Four of these options will result in a mean time between authentication failures substantially larger than the mean time between hardware failures.

The cryptologic aspects of the authentication process are treated in a classified annex, published separately.

Acc
NT ✓
DT
U
J.
By
Distrib tion/
Ava lability Codes
Dist
A

DTIC
COPY
INSPECTED
4

IDA PAPER P-1625

ROBUST AUTHENTICATION FOR THE NATIONAL SEISMIC SYSTEM

Joseph T. Beardwood

January 1982

INSTITUTE FOR DEFENSE ANALYSES
SCIENCE AND TECHNOLOGY DIVISION
1801 North Beauregard Street, Alexandria, Virginia 22311

Contract MDA 903 79 C 0202
DARPA Assignment A-64

ACKNOWLEDGMENTS

The author is indebted to Mr. Paul Stokes, Mr. William Golderick, and Mr. Dale Breding of Sandia Laboratories for providing a complete description of the prototype National Seismic System (NSS), a thorough understanding of system operations, and a history of system communications performance.

The author is also indebted to Mr. Dale Breding of Sandia Laboratories and Mr. John Woolston of Teledyne for providing the NSS data used to design and test the error-correcting algorithm described in Appendix B.

Finally, the author is grateful for the thoughtful, constructive reviews of the draft by Mr. James Bagnall, Dr. Gabriel Frenkel, Dr. Ostap Kosovych, and Dr. Raymond Pickholtz.

CONTENTS

FIGURES

TABLES

ABBREVIATIONS

ADC	Analog-to-Digital Converter
A/D	Analog-to-Digital
CONUS	Continental United States
CTB	Comprehensive Test Ban
CTBT	Comprehensive Test Ban Treaty
DARPA	Defense Advanced Research Projects Agency
DHSOH	Downhole State of Health
DOE	Department of Energy
GRA/ADC	Gain Ranging Analog-to-Digital Converter
LTBT	Limited Test Ban Treaty
LP	Long-Period (Signal)
MP	Mid-Period (Signal)
MTBAF	Mean Time Between Authentication Failures
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
MUX	Multiplexer
NSS	National Seismic System
PNE	Peaceful Nuclear Explosion

SCARS	Seismic Control and Recording Station
SOH	State of Health
SP	Short-Period (Signal)
TTBT	Threshold Test Ban Treaty
UHSOH	Uphole State of Health

I. INTRODUCTION AND SUMMARY

A. BACKGROUND

Although a treaty imposing a comprehensive ban on nuclear explosions has been on the international arms control agenda since the mid-1950s, no real progress toward a Comprehensive Test Ban Treaty (CTBT) was made until the mid-1970s. The most persistent barrier to such a treaty has been the issue of verifying compliance--agreeing to establish a system of control and inspection that could guarantee against secret testing.

The problems of monitoring compliance were first studied in the United States by the Bethe Panel in 1957 and 1958, and later examined in Geneva by an international Conference of Experts in 1958. Both studies concluded that to effectively monitor compliance with a CTBT it would be necessary to locate control posts, including seismic stations, throughout the territories of the treaty signatories, and that "highly mobile" inspection teams would be required to check out suspicious events.

Despite continuing negotiations between the U.S., the USSR, and the U.K., no solution appeared possible to the "in-country" monitoring and inspection problems, and, in fact, by 1963, the United States proposed to rely primarily on the detection capabilities of stations outside the USSR (Ref. 1), although it was recognized at the time that such a monitoring system could not protect completely against clandestine Soviet tests.

When President Carter placed a CTBT high on his list of priorities, negotiations were reinitiated between the

U.S., USSR, and U.K., in the fall of 1977. Twelve rounds of trilateral sessions were held, the most recent of which was recessed on November 11, 1980. Since a CTBT is not verifiable by national technical means alone, the United States has continued to press for effective supplementary measures. Significant progress has been made toward reaching agreement regarding on-site inspections and the use of a system of specially-equipped, tamper-proof seismic stations on the territories of the three parties.

Because the pace of the negotiations was rapid, and because early agreement seemed possible, the U.S. Department of Energy (DOE) tasked Sandia Laboratories (in October of 1977) to develop, on a crash basis, a prototype of what has been called the National Seismic System (NSS). The NSS was to include a prototype of the tamper-proof seismic stations and a Seismic Control and Recording System (SCARS) which would receive signals from the seismic stations by way of a satellite communications link, record this data for later analysis, and, in addition, issue commands to the seismic station for such functions as seismometer calibration. Sandia completed this Herculean task by October of 1978, and began continuous operations with the prototype seismic station* and SCARS in March, 1979. In August, 1979, a technical presentation concerning the prototype system, together with a demonstration of the hardware, was made to the Soviet negotiators in the United States.

*A description of the prototype system is given in Section II.

In anticipation of an early agreement on a CTBT, DOE kept Sandia and its subcontractors as suppliers on standby to manufacture seismic stations to be deployed on Soviet territory. When it became apparent that a CTBT was much lower on the Reagan Administration's priority list than it had been for President Carter, DOE terminated the NSS program and instituted two others in its place. The first of these, the Regional Seismic Test Network, calls for the deployment and operation of five NSS prototype stations, three in the U.S. and two in Canada, to discover any problems associated with the draft language describing the deployment of NSS stations should a treaty be concluded. The second program, the In-Country Seismic Program, is to gather inputs from all interested U.S. parties so as to produce a specification for a generic NSS--something impossible during the short time period allowed for development of the prototype system.

In the spirit of this latter program, one concern of the Defense Advanced Research Projects Agency (DARPA) has been that facet of the NSS design associated with making the seismic stations tamper-proof. To prevent the Soviets from substituting seismic data for those intervals of time during which signals from a Soviet test would reach the seismic stations, a cryptographic algorithm is used to derive an authentication word from the data to be transmitted. This word is compared with a second authentication word derived from the received data at SCARS, and, if a match occurs, the data is declared to be authentic. If the two words differ, the data is suspect. Such a scheme is susceptible to errors in transmission of the data, and should there be a large number of authentication failures, critical data may be declared suspect, or U.S. analysts could lose faith in the system. IDA was tasked by DARPA to examine this problem (see Appendix A).

B. STATEMENT OF ҐHE PROBLEM

Given that seismic data gathered by NSS stations is to be communicated in present time by satellite communications links to the U.S.-located SCARS, recommend operating techniques and/or equipment modifications (with regard to the prototype NSS) which will provide robust authentication for NSS signals. In effect, means were to be found which reduce to an acceptably low value the frequency of failures of authentication, resulting from bit errors introduced by the communications links. A goal of one year was set for mean time between authentication failures (MTBAF) resulting from errors introduced by the communication links, a figure matching the predicted mean time between failures (MTBF) for the NSS remote station hardware.

C. ASSUMPTIONS

A number of assumptions were used for analysis of NSS authentication. Several of these are political in nature since they concern the final agreements which may be reached among the U.S., USSR, and the U.K. on the design, deployment and operation of an NSS. Others represent a combination of political and technical issues concerning the ground and space segments of the NSS/SCARS satellite communication links. The final assumptions are purely technical in nature and reflect our opinion that drastic changes from the NSS prototype hardware are unlikely to occur.

1. Assumptions with Regard to Political Issues:

   a. That agreement will be reached between the parties (U.S., USSR., and U.K.) to deploy remote seismic sensing stations at locations to be specified by the monitoring countries. Specifically, the U.S. will be able to choose the approximate locations of stations deployed within the USSR to monitor compliance with a CTBT.

b. That the agreement to deploy stations of the NSS will contain the provision that data gathered by these stations will be transmitted, in present time, by commercial satellites to all of the signatories of a CTBT.

c. That the agreed-upon format for NSS data transmission will contain a provision permitting the inclusion of a small number of bits (one-half percent of the size of the data block), cryptographically derived from the data block, for authentication of received data--providing we supply proof of the true nature of these authentication bits. The proposed solution for USSR monitoring of the authentication bits is to provide the Soviets with cryptographic devices identical with those used in the NSS, and, in addition, provide them with the cryptovariables once they are no longer in use. In this way, the Soviets can calculate the authentication bits themselves, but would not be able to substitute false data because the cryptovariables provided would be out of date.

2. Assumptions with Regard to Satellite Communications Links:

a. That the CTB treaty signatories lease transponders of suitable characteristics on satellites at appropriate locations from INTELSAT and domestic satellite services.

b. That the reliability of the domestic satellites, mentioned above, is equal to, or better than that experienced by INTELSAT over the last few years.

c. That negotiations will be successfully completed with several countries (e.g., Australia and Japan) to provide, or permit the U.S. to contract with local corporations for the provision of and operation of earth terminals to relay satellite signals. Further, that the reliability of these stations is at least as good as that experienced over the last several years for the average terminal used with INTELSAT.

d. That the U.S. contracts with a domestic satellite carrier for earth stations in the U.S. that are as reliable or better than the average experienced for earth stations in use with INTELSAT.

e. That sufficient redundancy will be built into the SCARS satellite receiver that this unit will not contribute to link failures.

f. That failures in the ground stations of the NSS links are independent, and that failures in the satellites may be ignored.

3. Assumptions with Regard to Technical Issues:

a. That a single bit error in an NSS data frame will cause an authentication failure.

b. That the transmitter power and antenna gain of a generic NSS remote staton earth terminal will not differ from the 10 watts and 42.5 dB of the prototype system.

c. That symbol interleavers of depth one second will be used in conjunction with the Viterbi encoders and decoders.

d. That any error bursts encountered on the satellite links will last much less than one second so that the symbol interleaver will ensure independence of errors.

e. That the link budget for the generic NSS will be the same as that for the prototype system so that the probability of a bit error, after decoding, will remain 10^{-7} per hop.

f. That the NSS will not use switched ground circuits, and that three satellites will be required for connectivity between an NSS remote site and SCARS (e.g., USSR-Indian Ocean Satellite-Japan-Pacific Ocean Satellite-West Coast CONUS-Domestic Satellite-East Coast SCARS).

D. SUMMARY OF RESULTS

Nine options for NSS data communication were examined, using the assumptions stated above. These options were:

1. Current, on-line operation of the prototype NSS. No use is made of the 15-minute delayed transmission of data, and authentication is declared, if either of the authentication words computed at SCARS is identical to the corresponding received authentication word.
2. Compression of the NSS data frame, passing only the compressed frame through the authentication algorithm, appending the compressed frame to the original, and transmitting the combined frame to SCARS, where authentication words are computed from a locally compressed frame for comparison with the received authentication words.
3. Substitution, at SCARS, of data fields in an NSS received frame (data regeneration) with their à priori known content before computing authentication words, and application of an algorithm which corrects some errors in the received short-period data. No use is made of the 15-minute delayed transmission available in the prototype NSS.
4. Data regeneration using both the present time and 15-minute delayed transmissions available with the prototype system.
5. Use of both data regeneration and the short-period error correction algorithm with both the present time and 15-minute delayed transmissions with the prototype system.
6. Halve the data rate of the prototype system by eliminating the 15-minute delayed transmission, and use data regeneration at SCARS before computing the authentication words.

7. Use the one-half-rate data system with data regeneration, and also provide redundancy by using redundant earth stations in the satellite links connecting the remote stations and SCARS.
8. Full-rate transmission with the 15-minute delayed transmission replaced by a second, one-half-rate, forward-error-correcting encoder. Data regeneration to be used at SCARS before authentication.
9. Full-rate transmission with data regeneration and a second forward-error-correcting coder together with redundant ground stations for the remote station-SCARS satellite link.

The second option, that of using data compression to improve the MTBAF, was the originally-planned approach to the problem. Unfortunately, no compression scheme was discovered which could materially improve system MTBAF. Moreover, all of the compression schemes examined seriously degraded the system dynamic range necessary to detect hide-in-earthquake treaty evasion attempts. As a result, Options 3 through 9 were studied in an attempt to achieve robust authentication for the NSS.

For each option studied, we calculated not only the MTBAF, but also the average annual number of hours of NSS data that would have to be retrieved from the tape recorders* at the NSS remote stations. A summary of the results obtained is given in Table 1. The MTBAF ranges from a low of 0.39 hours (current on-line system) to an extreme of 10^{14} years. More interesting, however, is the fact the average annual time for which data

*For link outages of 15 minutes or less, loss of data is prevented through transmission of both present time and 15-minute delayed data frames. For outages longer than 15 minutes, however, tape recorders at the remote stations must be used to prevent data loss. These units, which record the delayed signal, are activated automatically when a remote station has not received command link signals for a period of 15 minutes. Presumably, recorded data would be retrieved on a monthly basis.

TABLE 1. MEAN TIME BETWEEN AUTHENTICATION FAILURES AND AVERAGE ANNUAL RECORDING TIME FOR VARIOUS NSS COMMUNICATION OPTIONS

OPTION	MTBAF	RECORDING TIME
Prototype as currently operated on-line	4.45×10^{-5} years (0.39 hrs)	32.8 hrs
Prototype with data regeneration and short-period error correction	1.43×10^{-4} years (1.25 hrs)	32.8 hrs
Prototype with data regeneration using both present time and 15-minute late transmissions	6.17×10^{-2} years (0.74 months)	32.8 hrs
Prototype with data regeneration, both transmissions, and short-period error correction	0.188 years	32.8 hrs
Data regeneration and halve the data rate by elimination of delayed transmission	4.7 years	39.0 hrs
Data regeneration, half data rate, and redundant earth stations	533 years*	10.25 min
Data regeneration, with delayed transmission replaced by a second forward error correcting code	10^{12} years*	39.0 hrs
Data regeneration, second code, and redundant earth stations	10^{14} years*	10.25 min

*It should be noted that these values are so large that they have no meaning in relation to an actual system life or deployment period.

must be recorded at each NSS remote station can be reduced from the 32.8 hours currently experienced to approximately 10 minutes.

In addition, note that the INTELSAT availability statistics used in this study (Ref. 2) are averages which include data from earth stations in third world countries--stations with notoriously poor maintenance records. Since none of these stations would be used for NSS communications, link outages are expected to be substantially less than those used to obtain the results presented here. In fact, if enough funds were made available for the NSS program, sufficient redundancy could be provided at the earth stations of the NSS/SCARS links to eliminate earth station outages as a cause of authentication failures.

E. CONCLUSIONS

Provided that symbol interleavers are used with the Viterbi encoders/decoders in the NSS satellite links to preclude burst errors, and provided that the NSS does not make use of switched terrestrial communications, it is possible to draw the following conclusions:

1. The MTBAF for the NSS can easily be made much longer than the one-year MTBF for the NSS hardware.
2. Use of redundant earth stations in the NSS/SCARS satellite links can materially aid in increasing the NSS MTBAF.
3. Use of redundant earth stations can reduce, to an almost negligible quantity, the information recorded at NSS remote stations to prevent loss of data during link outages.
4. Transmission of a delayed replica of the data is not satisfactory for reducing either reliance on tape recordings or lowering transmission errors.

5. Tape recorders at the remote stations need only be provided for failure of the NSS earth station, not the remainder of the communication link.

F. RECOMMENDATIONS

In light of the study results obtained, we make the following recommendations regarding the specifications for a generic NSS:

1. Symbol interleavers be used with the forward-error-correcting encoders/decoders.
2. No terrestrial switched lines be used in the NSS communication links.
3. The 15-minute delayed data be eliminated from the NSS NSS remote stations, and
4. The modems for NSS be modified so as to halve the data rate.
5. Redundant earth stations be used for all NSS data links.
6. That the SCARS authentication process be modified to make use of the redundant path transmissions provided by these redundant earth stations.
7. That NSS satellite links use non-switchable transponders (see Section IV).
8. Assuming no change in the authentication algorithm, that both 10-bit authentication words computed at SCARS be required to be identical with those received from a remote station to declare a data frame authentic, thus reducing the probability of successful data substitution to 10^{-6}.

II. DESCRIPTION OF THE PROTOTYPE SYSTEM

A. GENERAL

In order to consider methods of achieving robust authentication for the NSS, it is first necessary to examine the prototype system developed, essentially without specifications, by the Sandia Laboratories. An overall block diagram of this prototype system is given in Fig. 1. The borehole subsystem contains seismometers, filters, an A/D converter, and a digital processor that collects the seismic signals and converts them to digital form. It also gathers the downhole state of health (DHSOH) information in digital form, multiplexes this data with the seismic data, adds framing and timing information, and passes the combined data stream to the surface subsystem via an authenticator. A simplified block diagram of the borehole system is given in Fig. 2.

The uphole data subsystem, shown in Fig. 3, first merges uphole state of health (UHSOH) information with the borehole signals. It then creates a 15-minute delayed version of the real-time data with a digital delay line*, merges the delayed and real-time data streams, passes the merged data through a Viterbi rate one-half convolutional encoder, and finally transmits the encoded data to a satellite for relay to the U.S. SCARS. It should be noted that the NSS satellite terminal is not a standard INTELSAT earth station in that it has less

*Note that a digital tape recorder is used to avoid loss of data for communication link outages that persist for intervals longer than 15 minutes. Recording of the 15-minute delayed data is initiated by a 15-minute loss of signals from the command channel.

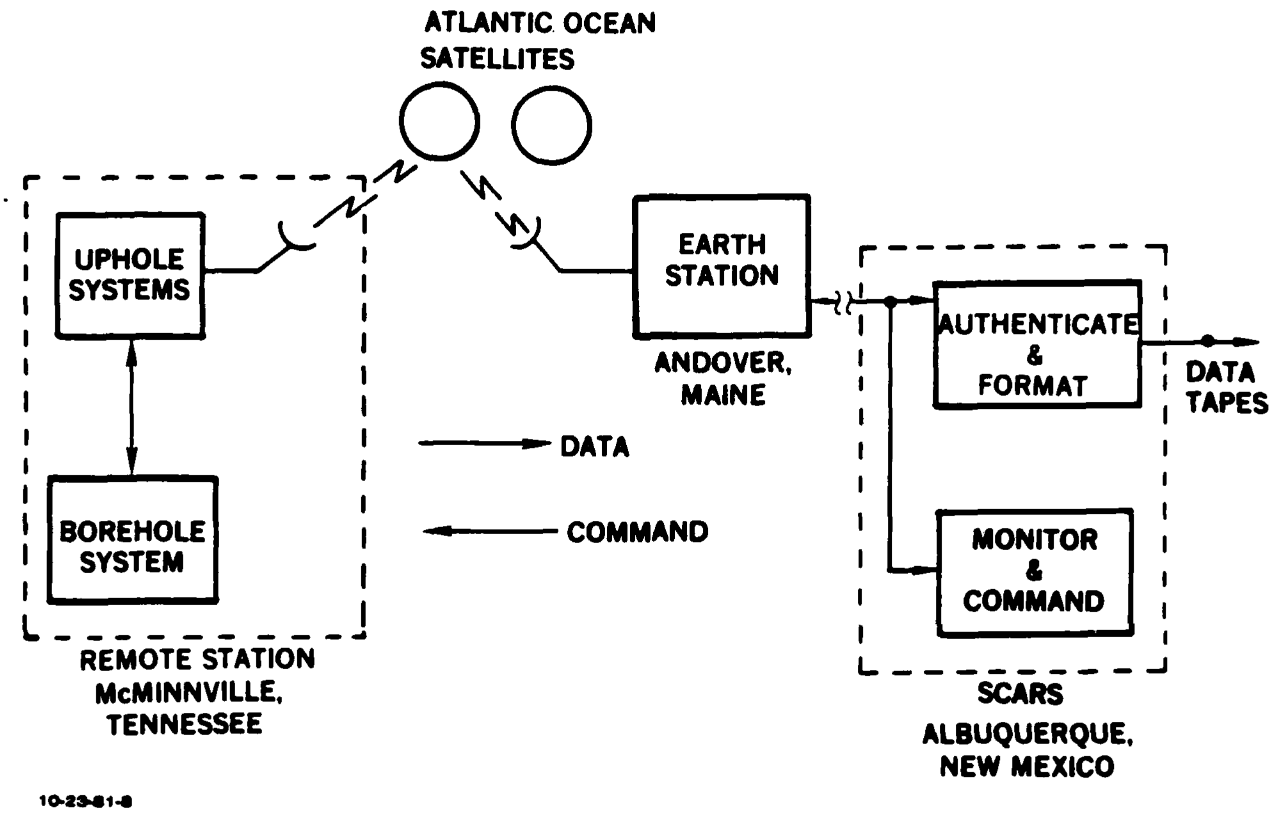
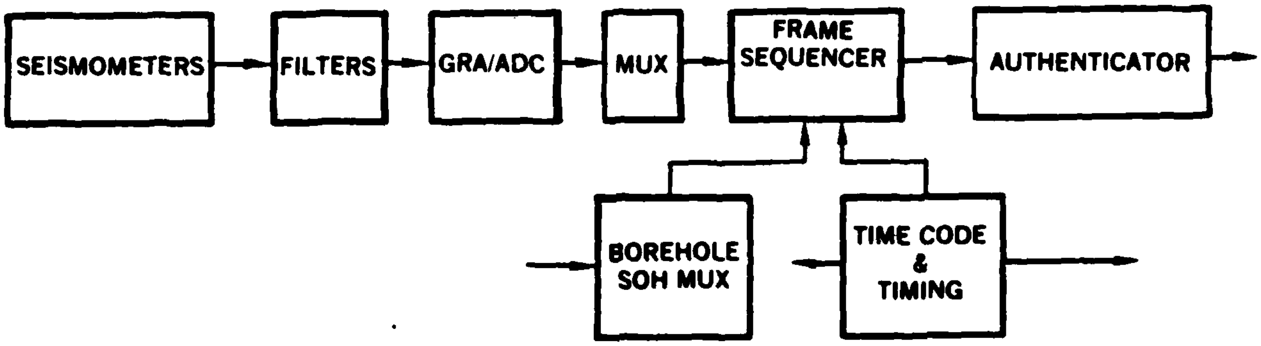


FIGURE 1. Prototype NSS



10-23-81-6

FIGURE 2. Prototype Borehole Data Systems

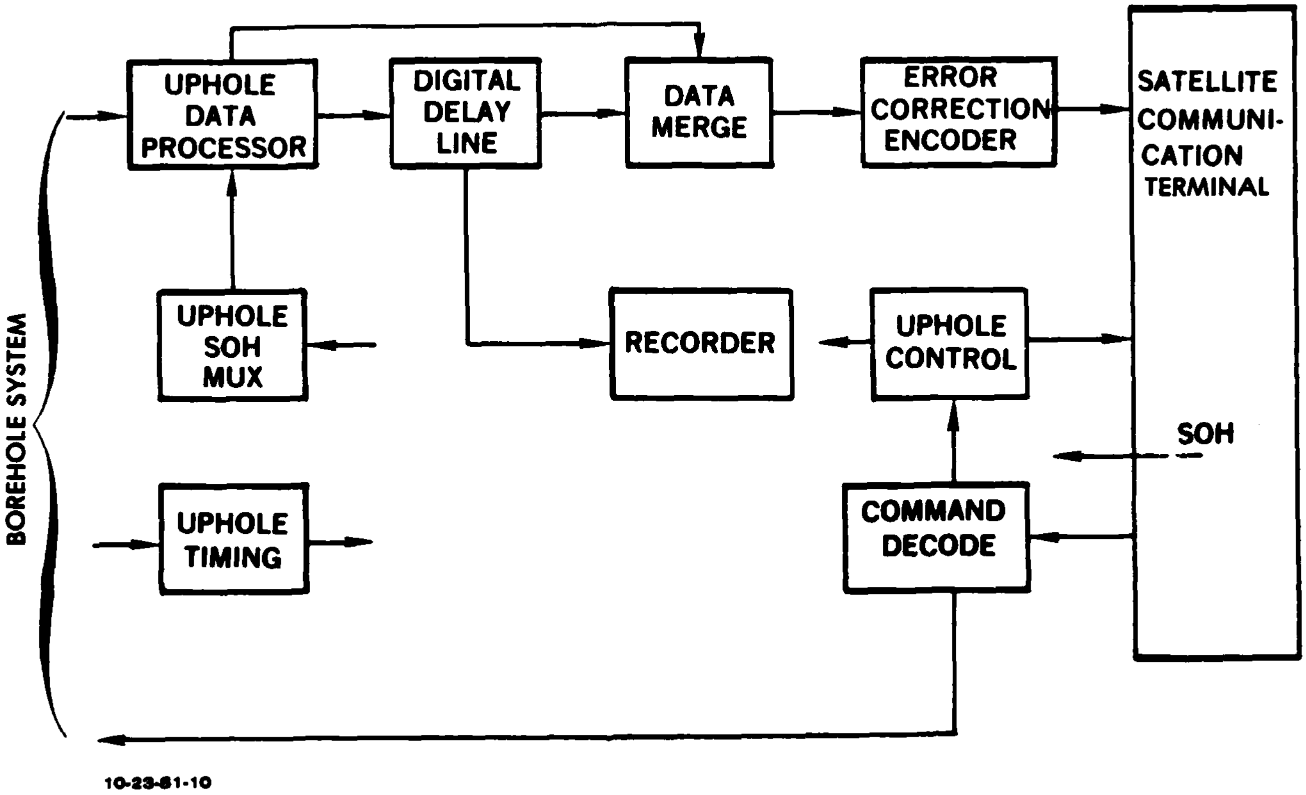


FIGURE 3. Prototype Uphole Systems

transmitter power (only 10 watts) and a small, non-tracking antenna (Ref. 3).

Because of the planned locations for the NSS remote terminals, east of the Caspian Sea and in the Kamchatka/Kuriles region, it is probable that two satellite links will be required to communicate NSS signals to CONUS. For example, the NSS stations located near the Caspian Sea could transmit signals to an Indian Ocean satellite. Signals from this satellite could be received by an earth terminal in either Japan or Australia, and relayed from that site to CONUS by way of a Pacific Ocean satellite.

After the NSS signals are received in CONUS, they must then be sent to the SCARS for processing. In all likelihood this last transmission will be via a domestic satellite (e.g., WESTAR) to avoid the burst errors and switching transients associated with the switched ground network. Finally, at SCARS the NSS data stream is reformatted and authenticated before analysis of the data takes place.

B. NSS DATA TRANSMISSION

1. Data Rate

The basıc seismic data to be transmitted from the NSS remote stations to the SCARS is derived from a single 3-axis (vertical, north/south, and east/west) seismometer (Geotech KS36000). The analog outputs of this seismometer are filtered to obtain Short-Period (SP), Mid-Period (MP), and Long-Period (LP) signals.* Since one of the two principal uses of the NSS is the detection, location, and identification of small explosion signals received simultaneously with signals from a large, nearby earthquake, it is important to provide both wide dynamic range and high amplitude resolution in the transmission of these signals. Because of state-of-the-art limitations of

*See Figs. 4, 5 and 6 for the frequency bands covered.

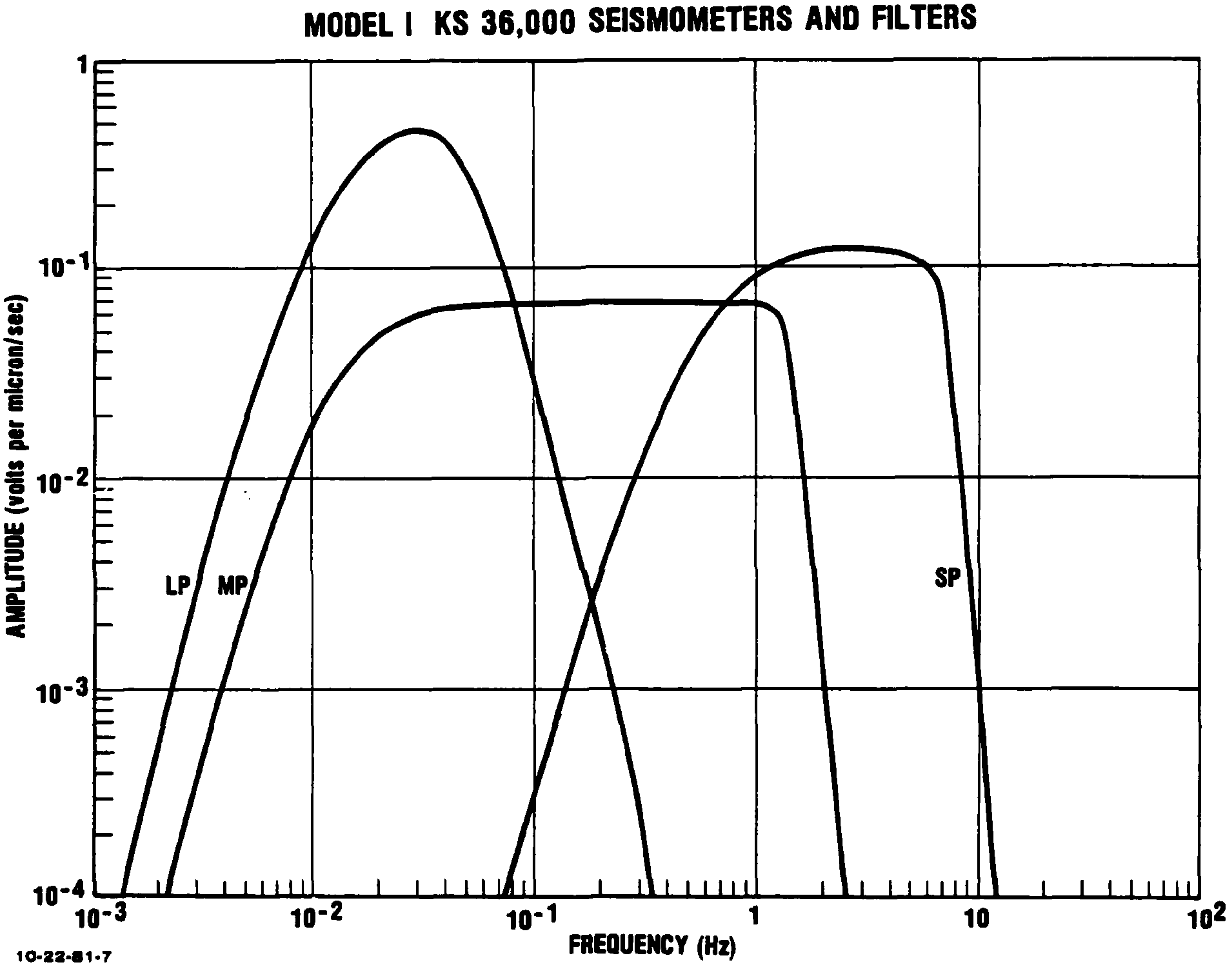


FIGURE 4. Vertical Response of the NSS Prototype System

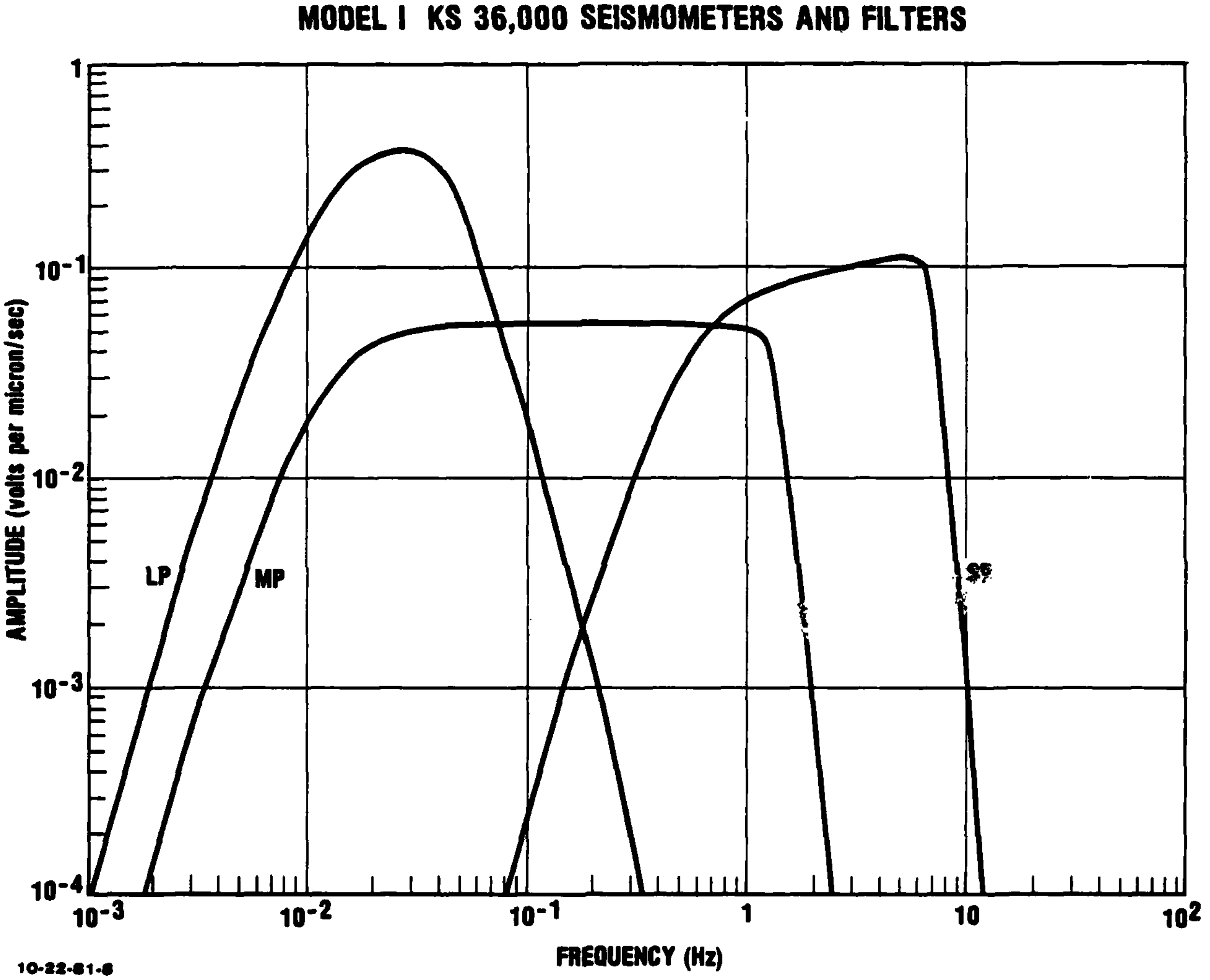


FIGURE 5. Horizontal Response of the NSS Prototype System

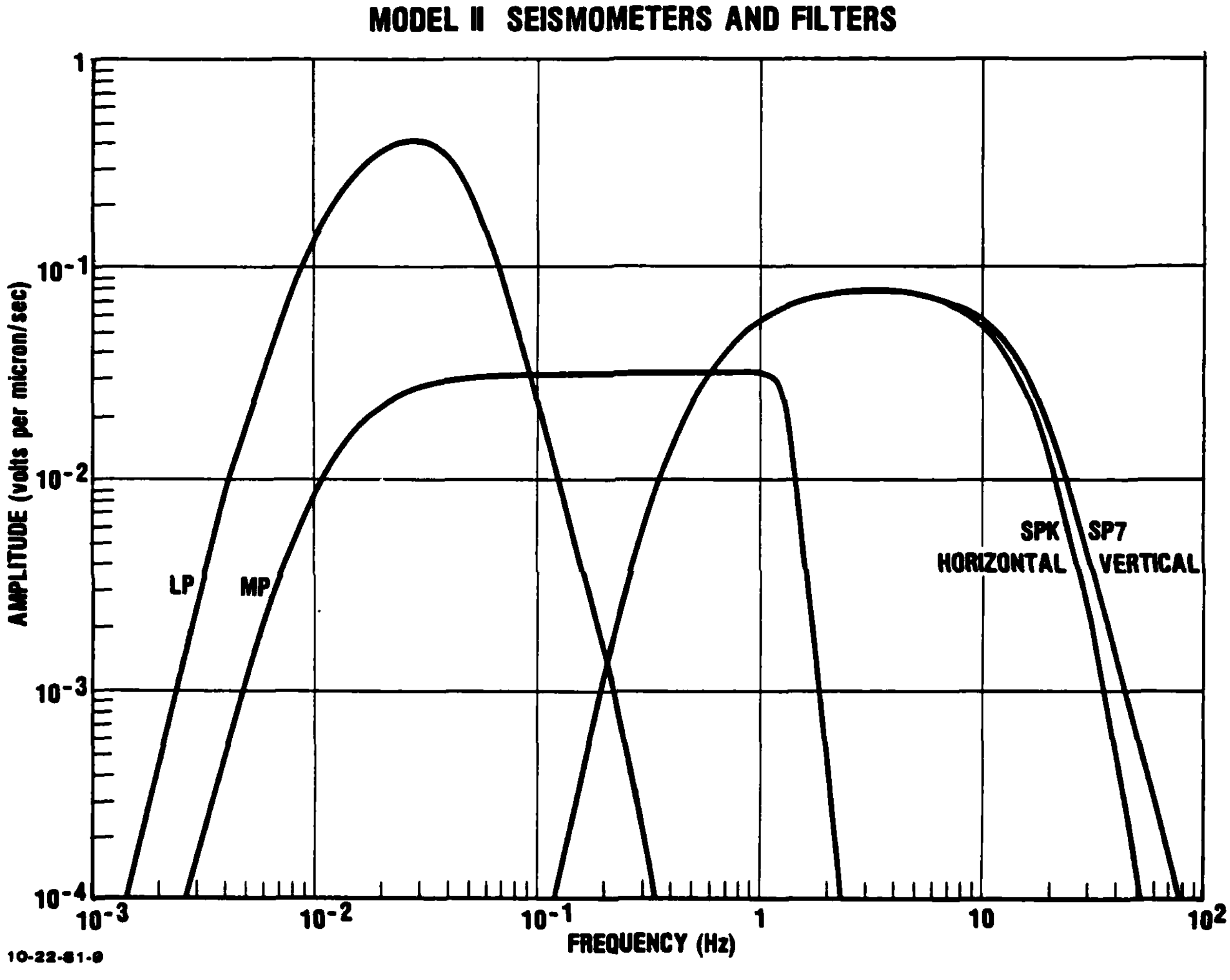


FIGURE 6. Modified Response of the NSS Prototype System

analog-to-digital converters (ADCs), samples of the nine (3 components each of SP, MP, and LP) seismic signals are converted to digital form using a 16-bit, gain-ranging ADC. The format of these digital samples is given in Fig. 7.

To preserve waveform fidelity for later analysis, each band is sampled at approximately four times the frequency of the upper 3 dB point of the system response for that band. Thus, the SP signals are sampled 40 times per second, the MP signals four times per second, and the LP signals once per second. Combining the digital seismic signals with fifteen 16-bit words containing a synchronization preamble, state of health, time, authentication words, etc., there are one-hundred and fifty 16-bit words of data generated each second. Taking into account time diversity (the real-time and delayed data streams) and forward-error-correction coding, the resultant data rate is 9,600 symbols per second, as shown in Table 2.

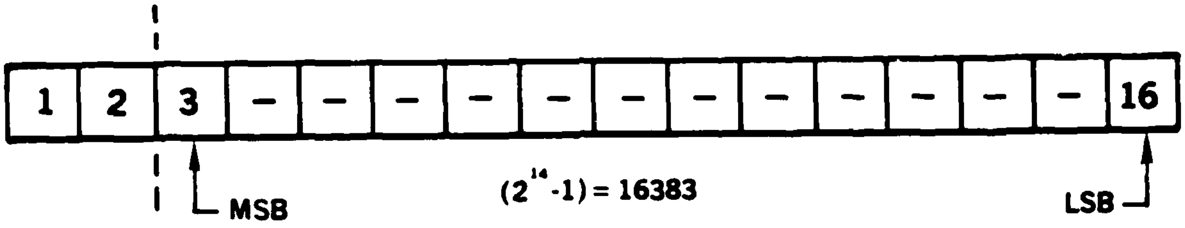
2. Transmission Format

Although the NSS data is transmitted in a continuous stream, it is logically broken into one-second frames. Each frame begins with a synchronization preamble, and ends with two authentication words as shown in Fig. 8. Note that each one second of data is authenticated.

3. Authenticator

As each one-second data frame is assembled by the borehole subsystem, the 130th 16-bit word of the frame, which will eventually contain the uphole state of health (see Fig. 8), is set to zero. The completed frame, less the two authentication words, is then passed through the authenticator which appends the two authentication words to the frame. The authenticator, shown in Fig. 9, actually consists of two* separate authenticators. Each of these authenticators performs a cryptologic

*The two authenticators differ only in that they use different cryptovariables.



- BITS 1 AND 2 = GAIN CODE = G_R

  00 = 128
  01 = 32
  10 = 8
  11 = 1

- BITS 3 THRU 16 = "RANGED" DATA LEVEL ESTIMATE = n_d

- "DE-RANGED" DATA LEVEL ESTIMATE = E_D

$$E_D = \frac{128}{G_R} \times 10^{-5} \times (n_d - 8191) \qquad \text{(volts)}$$

10-23-81-11

FIGURE 7. Analog-to-Digital Conversion Format

TABLE 2. NSS PROTOTYPE DATA RATES

3-AXIS LP	1 SAMPLE/sec	=	3	WORDS/sec	
3-AXIS MP	4	=	12		
3-AXIS SP	40	=	120		
			135		
SYNCH, STATION ID, SOH, etc.			15		
ONE DATA FRAME		=	150	WORDS/sec	
150 WORDS/sec X 16 BITS/WORD					2400 BITS/sec
TIME DIVERSITY MULTIPLEXING (X2)					4800 BITS/sec
FORWARD ERROR CORRECTION CODING (X2) (CONVOLUTIONAL, R = 1/2, K = 7)					9600 SYMBOLS/sec

| 16 BITS |

SYNC		TIME 1	CF1	SPN	SPE	SPZ	SPN	SPE	SPZ
	LPN	LPE	LPZ	"	"	"	"	"	"
				"	"	"	"	"	"
		COMMAND		"	"	"	"	"	"
	MPN	MPE	MPZ	"	"	"	"	"	"
				"	"	"	"	"	"
				"	"	"	"	"	"
				"	"	"	"	"	"
				"	"	"	"	"	"
	MPN	MPE	MPZ	"	"	"	"	"	"
				"	"	"	"	"	"
				"	"	"	"	"	"
				"	"	"	"	"	"
		DH/SOH	GT SOH	"	"	"	"	"	"
	MPN	MPE	MPZ	"	"	"	"	"	"
				"	"	"	"	"	"
				"	"	"	"	"	"
				"	"	"	"	"	"
		ARTIME	UH/SOH	"	"	"	"	"	"
	MPN	MPE	MPZ	SPN	SPE	SPZ	SPN	SPE	SPZ
	CF2	TIME 2	ID FA	AUTH 1	AUTH 2				

10-23-81-12

FIGURE 8. Prototype NSS Data Frame Format (one second, 2400 bits)

SYNC	Synchronization Preamble (32 bits)
TIME1	Lower 24 bits of system clock counter (24 bits)
CF1 & CF2	Command functions (e.g., noop, setup, execute) (8 bits)
SPN	Short-Period North Sample (16 bits)
SPE	Short-Period East Sample (16 bits)
SPZ	Short-Period Vertical Sample (16 bits)
LPN	Long-Period North Sample (16 bits)
LPE	Long-Period East Sample (16 bits)
LPZ	Long-Period Vertical Sample (16 bits)
COMMAND	Echo of Command Received from SCARS (32 bits)
MPN	Mid-Period North Sample (16 bits)
MPE	Mid-Period East Sample (16 bits)
MPZ	Mid-Period Vertical Sample (16 bits)
DH/SOH	Downhole state of health (16 bits)
GTSOH	Seismometer state of health (16 bits)
ARTIME	Arrival Time of last command (16 bits)
UH/SOH	Uphole state of health (16 bits)
TIME2	Lower 20 bits and bits 25-28 of system clock counter (24 bits)
ID	Station Identification number (8 bits)
FA	Fixed pattern (11111010) (8 bits)
AUTH1 & 2	Authentication words (16 bits)

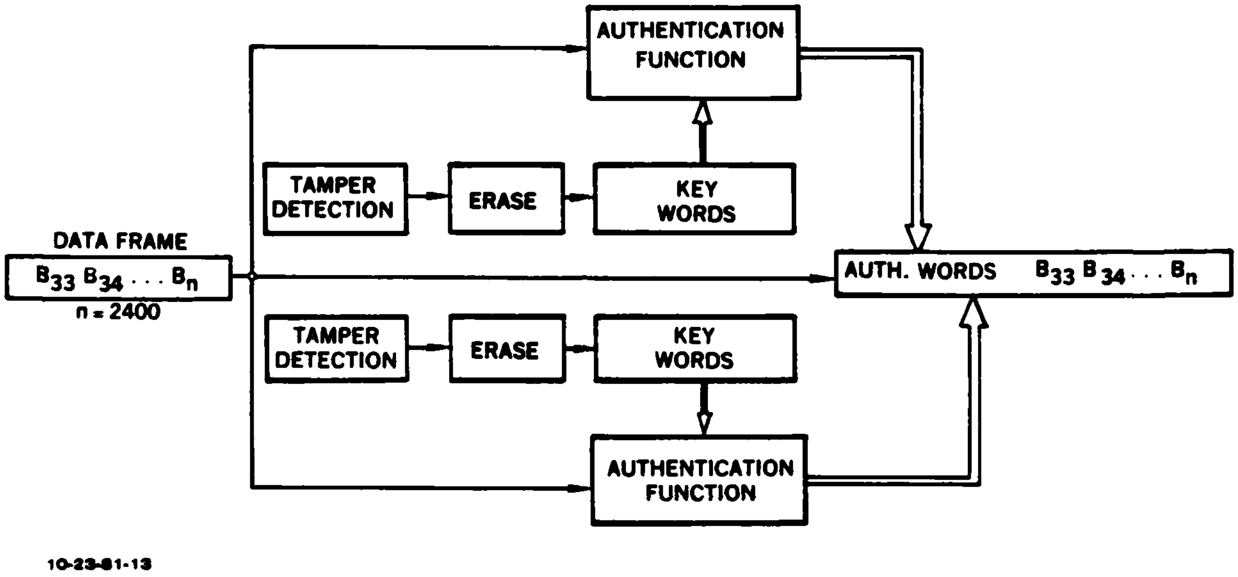


FIGURE 9. NSS Authenticator

mapping* of the 2368 data bits into 10 bits which are entered as the ten least significant bits of an authentication word with the remaining bits set to zero. Once the data frame reaches the uphole system, the uphole state of health information is substituted for the 130th word in the data frame by the borehole system and the frame is passed to the time redundancy and forward-error-correction encoder before transmission to the SCARS.

Once a data frame is received at the SCARS, a copy is made of the frame with the uphole state of health word set to zero and the authentication words removed. This modified frame, which should be identical to that generated by the remote site borehole system before the authentication words were appended, is then processed by an authenticator at the SCARS with the same cryptovariables used at the remote site authenticator. The two 10-bit words generated by the SCARS authenticator are compared with the appropriate bits in the authentication words of the received frame, and if either is a match authentication is declared for that frame.

It should be pointed out that the mapping process employed by the authentication algorithm has none of the properties of the mapping process used to obtain the check bits for an error detection encoder. The authentication algorithm simply produces, in an unpredictable manner, one of the 1024 possible 10-bit patterns for each input frame such that, with each frame containing different data, the distribution of 10-bit patterns is uniform. The result of the process is that an enemy attempting to substitute different seismic data will have one chance in 1024 that the SCARS will accept the frame as authentic. On the other hand, single-bit errors introduced in the communications channel will not always cause a frame to fail authentication.

*See Addendum A for a discussion of the authentication algorithm.

It is not clear, probably because of the crash nature of the development program, how the prototype design chose either 10-bit authentication words or chose to use two of them per frame while 32 bits are available for the transmission of authentication bits. From a communications viewpoint, if we assume random errors, a frame will not authenticate if there is an error in the data or an error in each authentication word or errors in both. As will be shown in Section III, the contribution of bit errors in the authentication words, toward failure to authenticate, is negligible, and we will concern ourselves solely with errors in the data.

III. TECHNICAL DISCUSSION

A. INTRODUCTION

For the following discussion, it is assumed that data collected at the remote seismic stations of the NSS will be transmitted to the SCARS in the clear, and that a small number of bits, cryptographically derived from this data (a single authentication word), will be appended to it so that the SCARS may authenticate the received data. The authentication process, at SCARS, consists of comparing the received authentication bits with ones derived from the received data using the same cryptovariables employed at the remote station. If the received and locally-derived authentication bits are identical, the data is declared authentic. If they differ by even one bit, the data is declared suspect.

Since all digital communications links are subject to errors, NSS data may fail to authenticate when the data or authentication bits are received with transmission errors.* The objective of this study was to reduce the number of communication error-induced authentication failures to an acceptable level in the simplest and least costly manner. Assuming that bit errors in the communication channel are random and of low probability, we will choose the mean time between authentication failures (MTBAF) as a figure of merit, and attempt to

*In the cryptologic mapping of n data bits into m authentication bits, there are 2^{n-m} data patterns which produce the same pattern of authentication bits. Further, since the mapping has a minimum Hamming distance of zero, single-bit changes in the data do not always alter the pattern of authentication bits produced.

achieve an MTBAF which equals, or exceeds, the one-year mean time between failures for the NSS remote station hardware (Ref. 4).

For discussion purposes, let us divide the NSS data into one-second blocks. An authentication word containing approximately 100 times fewer bits than the data block will be appended to this block with the total called a frame. We will then assume that a given frame will fail to authenticate if there are bit errors in either the data block or the authentication word.* We also assume that interleavers are inserted between the encoder/decoder and the modems to eliminate any possibility of burst errors on the communication channel. Thus, an upper bound on the probability that a given NSS frame will fail to authenticate is:

$$P_{FA} \leq 1 - (1 - P)^{Nd} (1 - P)^{Na} \qquad (1)$$

where: P is the probability of a bit error
Nd is the number of bits in the data block
Na is the number of bits in the authentication word.

If we assume $P < 10^{-5}$, Eq. (1) may be approximated by

$$P_{FA} \simeq 1 - (1 - NdP)(1 - NaP) \simeq (Nd + Na)P \qquad (2)$$

and, with the assumption that Nd >> Na

$$P_{FA} \simeq NdP \qquad (3)$$

and

$$MTBAF = 1/P_{FA} \simeq (NdP)^{-1} \text{ (seconds)} \quad . \qquad (4)$$

*See footnote on previous page.

Before proceeding, it is necessary to note that a three-hop satellite link will be required to transmit data from the remote NSS stations to the SCARS (see Fig. 10). At each ground relay station, the data will be converted to baseband, error corrected and reencoded before retransmission. For this case, assuming independent errors on each hop of the link, the probability of a bit error in the data received at SCARS will be

$$P = 3p$$

where: p is the probability of a bit error on a single hop. For the prototype system, as now operated on-line, Nd = 2352 and $p = 10^{-7}$ (Ref. 3). Thus, $P = 3 \times 10^{-7}$ and

$$\text{MTBAF} \simeq 0.39^{*} \text{ hours,}$$

more than four orders of magnitude short of our one-year goal.

It should be noted that the MTBAF given above applies only for that period of time when the remote station/SCARS channel is available. For 1982, we would have expected no connectivity for approximately 38.9 hrs (see Appendix D).

B. OPTIONS FOR INCREASING MTBAF

1. Data Compression

The original program plan (see Appendix A) called for a review of data compression schemes, suitable for seismic waveforms, with the objective of materially reducing Nd. The hope was to find a representation of a one-second waveform such that it would require only several percent of the number of bits presently used to represent NSS waveforms. In addition, the compression algorithm was to be relatively insensitive to

*Measured MTBAF for the McMinnville, Tennessee prototype is nearly two orders of magnitude larger than this calculated value. The discrepancy is undoubtedly the result of less intermodulation interference from other users of the same satellite transponder than allowed for with the 6.2 dB margin in signal-to-noise ratio of the prototype design (see Ref. 3).

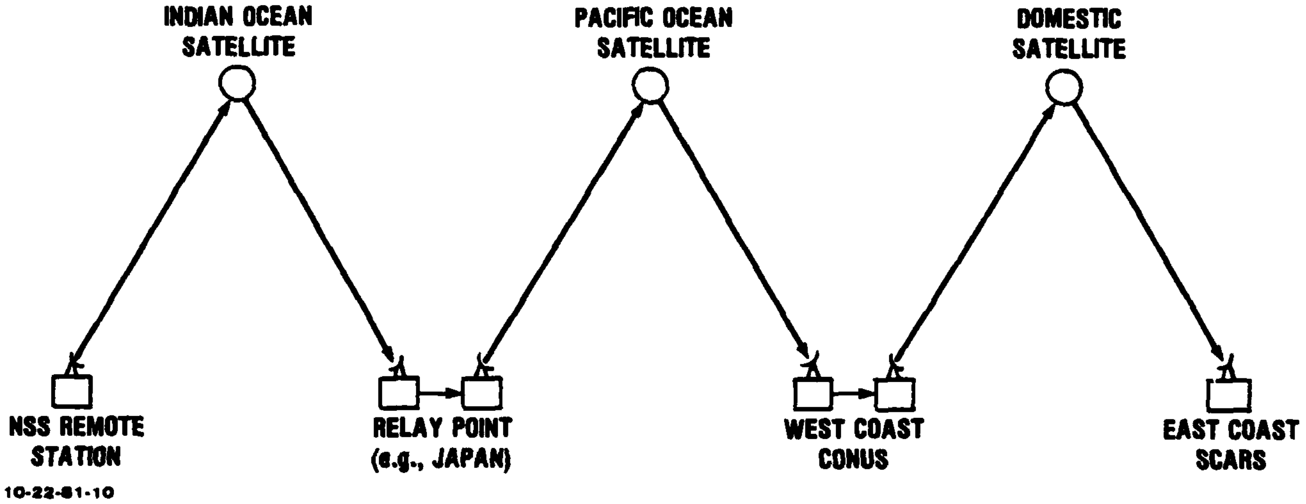


FIGURE 10. Representative NSS Satellite Link

occasional bit errors in the original data. If such a compression scheme could be found, only the new representation was to be passed through the authenticator. The transmitted signal would then include not only the original data and the authentication word, but also the compressed data as well. At SCARS, the received data were to be compressed in the same way as to the remote station, passed through a similar authentication algorithm, and the received and SCARS-generated authentication words compared.

A diligent search of the literature (see Bibliography) failed to discover any algorithm suitable for the purpose. Most of the compression schemes reviewed require a great deal of redundancy and known signal structures (e.g., voice compression) to operate effectively. While these requirements could readily be met for NSS teleseismic signals, they could not be met for the important case of near regional signals where the Nyquist rate of the seismic signals approaches the sampling rate for the system. On the other hand, compression schemes not requiring data redundancy (e.g., video compression) do not provide large compression ratios (factors of two to four), and result in a signal-to-coder generated noise ratio of 20 dB or less. This figure is clearly incompatible with the NSS dynamic range of 100+ dB necessary to detect and identify small explosion signals received simultaneously with those from a large earthquake during a hide-in-earthquake evasion attempt.

In any case, even if a useful compression ratio of 100:1 was possible, we would still be short of our one-year MTBAF goal by a factor of approximately 300. It was agreed, therefore, to pursue other options for increasing the MTBAF.

2. Data Regeneration at SCARS and Use of the Redundant Transmission

Our first step was to examine what improvements are possible with the prototype NSS design through regeneration, at SCARS, and replacement of data fields in an NSS frame which are known à priori, or can be reliably predicted at SCARS and, in addition, make use of the 15-minute delayed data as well as that transmitted in present time.

It is possible to reduce the number of data bits that can contain errors from the 2352 figure used in Section II to 2256 (see Table 3). The synchronization preamble and the trailing ID/FA words of the frame are identical from frame to frame, and the two 24-bit fields TIME1 and TIME2 (see Fig. 8) are the outputs of a downhole counter driven by a clock stable enough so that the counter output may be predicted, even after several hours outage of the satellite link. These 96 bits of the data block may be regenerated at SCARS, and thus removed as sources of error before authentication. To employ the redundant data transmissions, we first note that the probability of a frame not authenticating when there are two independent transmissions, P_{FAR}, is simply the square of the probability of failure for only one transmission. Thus,

$$F_{FAR} \simeq (Nd\ P)^2 \ . \qquad (5)$$

For most of the time both the current and 15-minute delayed data will be received at SCARS. During link outages of less than 15 minutes, only one of the two transmissions will be available, and for link outages 15 minutes or longer, neither neither signal will be received. To calculate the MTBAF for periods during which some link data is available, we first calculate the expected number of failures during a year, $\hat{N}_{TF}$:

$$\hat{N}_{TF} = \hat{N}_{SDF} + \hat{N}_{RDF} \qquad (6)$$

where $\hat{N}_{SDF}$ is the expected number of failures with one transmission available, and

$\hat{N}_{RDF}$ is the expected number of failures with both transmissions available

TABLE 3. NSS DATA FRAME BITS SUBJECT TO AUTHENTICATION

DATA DESIGNATION*	NUMBER OF BITS	
TRANSMITTED FRAME	2400	
AUTHENTICATION WORDS	-32	Not part of the data to be authenticated
UH/SOH	-16	Set to zero before authentication
	2352	Currently authenticated
SYNCH	-32	known à priori at SCARS and may be substituted for the received bits
ID/FA	-16	
TIME1	-24	
TIME2	-24	
	2256	bits subject to transmission errors

*See Fig. 8.

now

$$\hat{N}_{SDF} = NSDL \times P_{FA} \tag{7}$$

and

$$\hat{N}_{RDF} = NRDL \times P_{FAR} \tag{8}$$

where NSDL is the average number of frames per year for which only one transmission is received, and
NRDL is the average number of frames per year for which both transmissions are available.

From Appendix C,

$$NSDL = 5{,}475\ n \tag{9}$$

and

$$NRDL = 31{,}536{,}000 - 34{,}970\ n \tag{10}$$

where n is the number of ground stations in the link.

For the three-hop link we have hypothesized, we will assume that the SCARS will have sufficient redundancy that its receiver need not be counted in the failure statistics. Thus, the number of ground stations will be four, as shown in Fig. 10. Then, with Nd = 2256 and $p = 10^{-7}$,

$$\hat{N}_{TF} \quad 14.83 + 14.38 \simeq 29.21$$

and

$$MTBAF = (\hat{N}_{TA})^{-1} \simeq 0.41 \text{ months}$$

and, from Appendix C, there will be 32.8 hours per year which must be tape recorded (link outage time greater than 15 minutes). While this value of MTBAF is a substantial improvement over the 0.39 hours predicted for the prototype system as currently operated, it is still orders of magnitude less than our goal.

3. Correction of Errors in the Received Short-Period Data

While no suitable data compression scheme was found, it is possible to make use of the fact that while short period channels of NSS data are sampled at a 40 Hz rate, the signals in these channels have no appreciable energy for frequencies above 10 Hz.* An algorithm has been developed that can correct 80 percent of single bit errors in any of the three short period channels provided that the error occurs in the center second of an otherwise error-free, three-second block. As shown in Appendix B, use of this algorithm, together with the data regeneration and substitution previously described gives:

$$\text{MTBAF} \simeq 1.25 \text{ hours (no redundancy)}$$

and

$$\text{MTBAF} \simeq 0.188 \text{ years (use redundancy).}$$

While the MTBAF using the error-correction algorithm with redundancy is more than three times that using redundancy alone, it is only a fraction of our goal, and there will be an average of 32.8 hours of data per year that will have to be recovered by retrieving data tapes from the NSS stations. This would require, in our estimation, monthly visits to all 10 remote sites. Moreover, this performance can be achieved only by using the bubble memory digital delay line which has been declared unexportable. The correction algorithm could be used, however, in other modes of operation if required.

4. Reduced Data Rate with Redundant Ground Stations

Assuming the bubble memory is deleted from the prototype design, and the delayed data transmission with it, the system data rate would be halved. This in turn would lead to a 3 dB increase (with suitable modem modifications) in E_b/N_o. From Fig. 11, which shows the theoretical performance for the Viterbi decoder used in the prototype system (Ref. 5), we see that a 3 dB increase in E_b/N_o over that necessary for a

*Except for those rare intervals when signals are being received from very nearby seismic disturbances.

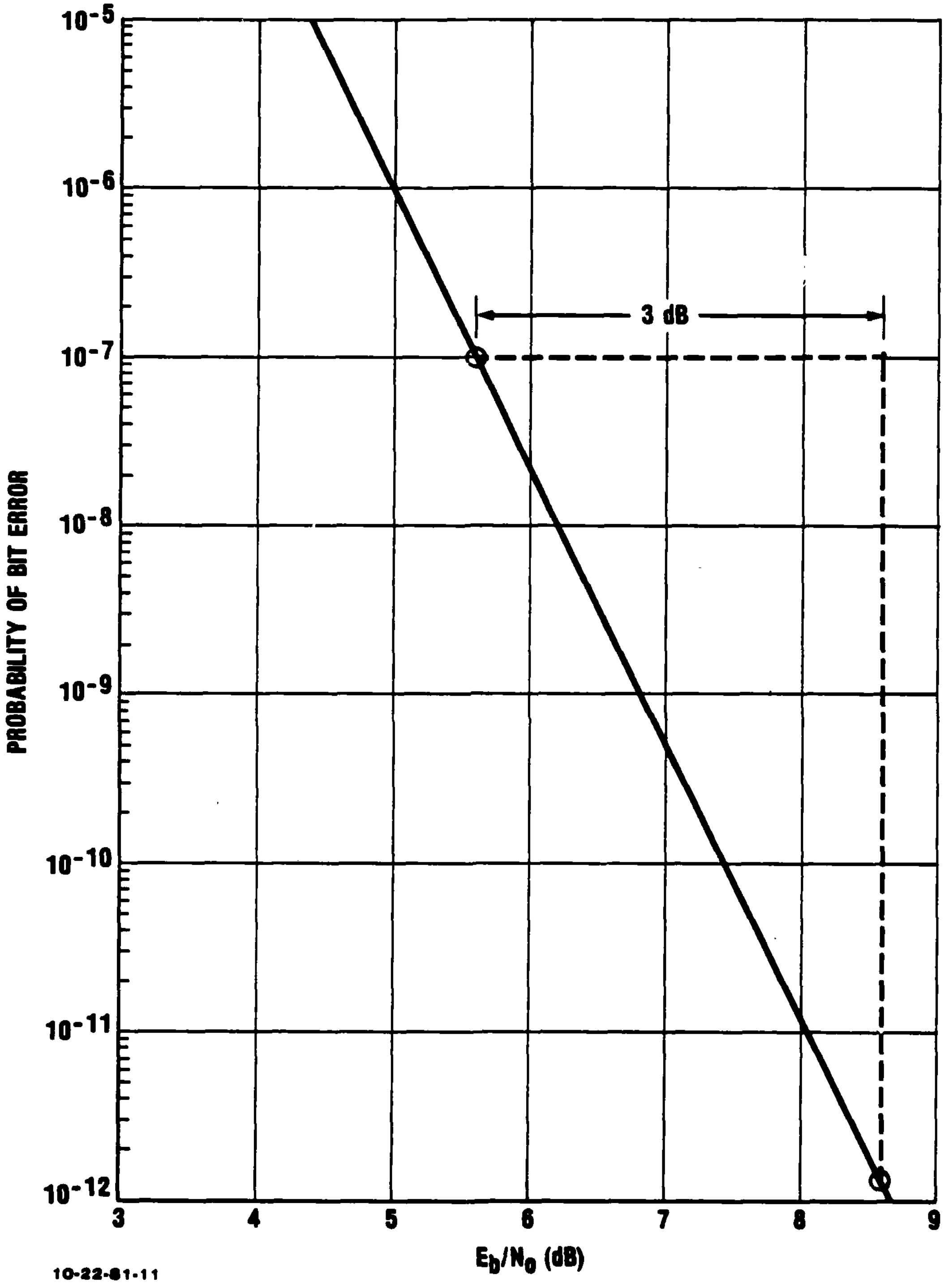


FIGURE 11. Theoretical Performance of Viterbi Rate 1/2, K=7, 3-bit Quantization Decoder

probability of bit error of 10^{-7} will lower this probability to 10^{-12}. With $N_d = 2256$, the MTBAF will be approximately 4.7 years, a value which exceeds our one-year goal. There will be, however, nearly 39 hours/year for which no link data will be available. This latter problem, however, can be greatly lessened if we resort to redundant ground stations for the NSS satellite links. In this case, as shown in Appendix D, the average total duration of link outages will be 10.25 minutes/year. If, in addition, we make use of the redundant signal paths provided, the MTBAF would become 533 years.

5. Concatenated Encoders with Redundant Ground Stations

One further option was examined. With the removal of the 15-minute late transmission, a second forward-error encoder (rate 1/2, feedback code) could be used withou increasing the data rate over that employed by the prototype system. The probability of a bit in error with the concatenated codes (P') for small probability of error with the Viterbi code alone (P), can be approximated by (Ref. 6):

$$P' \simeq 2000\ P^4.$$

Then, if we retain the redundant ground station configuration described above, for p (single hop with Viterbi code alone) = 10^{-7}, the MTBAF becomes approximately 10^{12} and 10^{14} years for the non-redundant and redundant authentication processors, respectively.

IV. COMMENTS REGARDING NSS SATELLITE LINKS

Neither the transmission of seismic data from the NSS remote stations to SCARS nor the transmission of commands from from SCARS to the remote stations fall within INTELSAT's definition of telecommunications. As a result, both the data and command links of the NSS must be treated as special services. INTELSAT has determined that special services can be supplied through the lease of at least one-quarter of a space segment transponder.

Transponders may be leased on two bases: dedicated or switchable. Although the cost for a dedicated transponder is some 4.7 times that for a switchable transponder ($2.8 million/yr versus $600,000/yr), it is essential that the NSS choose a dedicated transponder. For example, the prototype NSS, using an R&D, switchable transponder on an INTELSAT satellite lost communications for three-hour periods for several nights in March, 1979, when the finals of the NCAA basketball tournament were being broadcast to Europe via the satellite (Ref. 7). These outages were predictable well in advanced, and thus could have been used to detonate a Soviet test.

Further, by placing all NSS links in a single transponder with no other users, it will be possible, except for intentional jamming of the satellite, to control the link budget for that transponder completely within the U.S. In this way it will be possible to prevent excessive intermodulation interference from other users of the transponder.

REFERENCES

1. Carl F. Romney, Testimony before the Joint Committee on Atomic Energy, Congress of the United States, March 1963.

2. INTELSAT System Status Report for Deember 1978, Addendum No. 1 to BG-37-4E W/3/79.

3. K. Green, et al., "Automatic Seismic Observatory Communications System," COMSAT Technical Review, Vol. 10, No. 1, Spring 1980.

4. Sandia Corporation, "NSS National Seismic Station," Technical Presentation, August 1979.

5. Joseph P. Odenwalder, "Error Control Coding Handbook," Final Report on Contract F44620-76-C-0056, Linkabit Corporation, 15 July 1976.

6. A.J. Viterbi, private communication.

7. W. Goldrick, Sandia Laboratories, private communication.

8. George Lawler, Assistant General Manager, International Communications, COMSAT Corporation, private communication.

BIBLIOGRAPHY ON DATA COMPRESSION

H.R. Schindler, "Delta Modulation," IEEE Spectrum, Vol. 7, pg. 69, October 1970.

F.B. Johnson, "Calculating Delta Modulator Performance," IEEE Trans. Audio Electroacoustics, Vol. AV-16, pg. 121, March 1968.

H.W. Adelmann et al., "An ADPCM Approach to Reduce the Bit Rate of μ-Low Encoded Speech," BSTJ, Vol. 58, No. 7, pg. 1659.

D. Mitra, B. Gotz, "An Adaptive PCM System Designed for Noisy Channels and Digital Implementations," BSTJ, Vol. 57, No. 7, pg. 2727, September 1978.

W. Boyce, "Step Response of an Adaptive Delta Modulator," BSTJ, Vol. 55, No. 4, pg. 373, April 1976.

N.S. Jayant, "Adaptive Delta Modulation with a One-Bit Memory," BSTJ, Vol. 49, No. 3, pg. 321, March 1970.

J.E. Abate, "Linear and Adaptive Delta Modulation," Proc. IEEE, Vol. 55, pg. 298, March 1967.

M.R. Aaron et al., "Response of Delta Modulation to Gaussian Signals," BSTJ, Vol. 48, pg. 1167, May-June 1969.

M.R. Winkler, "Pictorial Transmission with HIDM," 1965 IEEE International Convention Record, Pt. 1, pg. 260.

APPENDIX A

TASK STATEMENT--PROJECT ASSIGNMENT A-64

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
1400 WILSON BOULEVARD
ARLINGTON VIRGINIA 22209

ASSIGNMENT FOR WORK TO BE PERFORMED
BY
INSTITUTE FOR DEFENSE ANALYSES

PROJECT ASSIGNMENT A-64 DATE: 2 9 DEC 1980

You are hereby requested to undertake the following task:

1. TITLE: Seismic Data Authentication

2. BACKGROUND: The United States employs seismic stations at a number of overseas locations to monitor underground nuclear tests by foreign nations. This network of stations supports technical intelligence activities, is used to monitor compliance with the Threshold Nuclear Test Ban Treaty (unratified), and will be used to monitor compliance with the Comprehensive Nuclear Test Ban Treaty now being negotiated with the Soviet Union.

The geographic distribution of these seismic stations was chosen to be both near to, and surround potential nuclear test sites. As a result, many of these stations are located in or near seismically active regions. To make sure that signals from large, nearby earthquakes do not obliterate signals from small explosions, the system employs an extremely large dynamic range (>120 dB). Digital communications are used to preserve this dynamic range during transmission from these stations to a U.S. analysis center, with the seismic signals being digitized directly at the seismometers.

Because of the geographic locations of the stations of detection network, many of the communications links are not under U.S. control. There exists, therefore, the opportunity for potential test ban evaders to substitute for, or alter data from the seismic sensors for those periods of time during which signals from a clandestine test would be received. It is necessary, therefore, to provide a means of authenticating the seismic data received at the analysis center.

The present approach to authentication involves redundancy, an NSA supplied authentication algorithm, and forward error correcting coding. This authentication procedure has two shortcomings. First, it more than quadruples the signaling rate over that needed to transmit the seismic data alone. Second, even with a low bit error rate in the communications channel, there are many blocks of data which are not authenticated. While it may be possible to tolerate the current amount of unauthenticated data, the bandwidth expansion will become intolerable as some of the stations with arrays of seismometers require data authentication. As a result, it is important to develop authentication means which minimize the expansion of required signaling rate. It is also desirable to reduce the quantity of unauthenticated data resulting from bit errors in the communication channel. The suggested means of achieving both results is to make use of the inherent characteristics of the seismic signals themselves.

3. OBJECTIVE: This study will examine data compression, as it applies to seismic signals, with the view of characterizing short intervals of seismic signals (typically several dominant periods) by a few, medium precision (∿8 bits) coefficients. The study would then examine how these coefficients, together with an authentication algorithm for these coefficients alone, could be concatenated with the seismic signals to provide authentication of the seismic data received at the analysis center.

4. SCOPE: The study will make use of previous work in several fields, and add to it in attempting to find a robust, low overhead procedure for authentication of seismic data. The study will concern itself with the following topics:

a. Review previous work in data compression, particularly as related to seismic data,

b. Review previous work in authentication of digital communications,

c. Design of several compressional algorithms using DARPA supplied seismic data (in digital form) and the information developed in a above, and

d. Use additional seismic data, provided by DARPA, to test the efficacy of these algorithms in conjunction with authentication algorithms, developed in b above, and forward error correcting codes in providing a robust authentication scheme which adds minimally to overhead in the digital transmission of seismic data.

5. SCALE OF EFFORTS: Expenditure of $100,000 of FY 81 funds is authorized for this task.

6. SCHEDULE: This study will commence on 1 December 1980. A draft final report shall be delivered to the cognizant office by September 15, 1981.

7. TECHNICAL COGNIZANCE: Assistant Director (Nuclear Monitoring Research), Defense Sciences Office, DARPA.

8. REPORT DISTRIBUTION AND CONTROL: The Assistant Director (NMR), DSO, DARPA, will determine the number of copies of reports and their distribution. A "need-to-know" is hereby established in connection with this task, and access to classified documents and publications, security clearances and the like, necessary to complete the task, will be obtained through the Director, DARPA.

Carl F Romney
for Robert R. Fossum
Director

ACCEPTED: Alexander H Flax
Alexander H. Flax
President, IDA

DATE: November 6, 1980

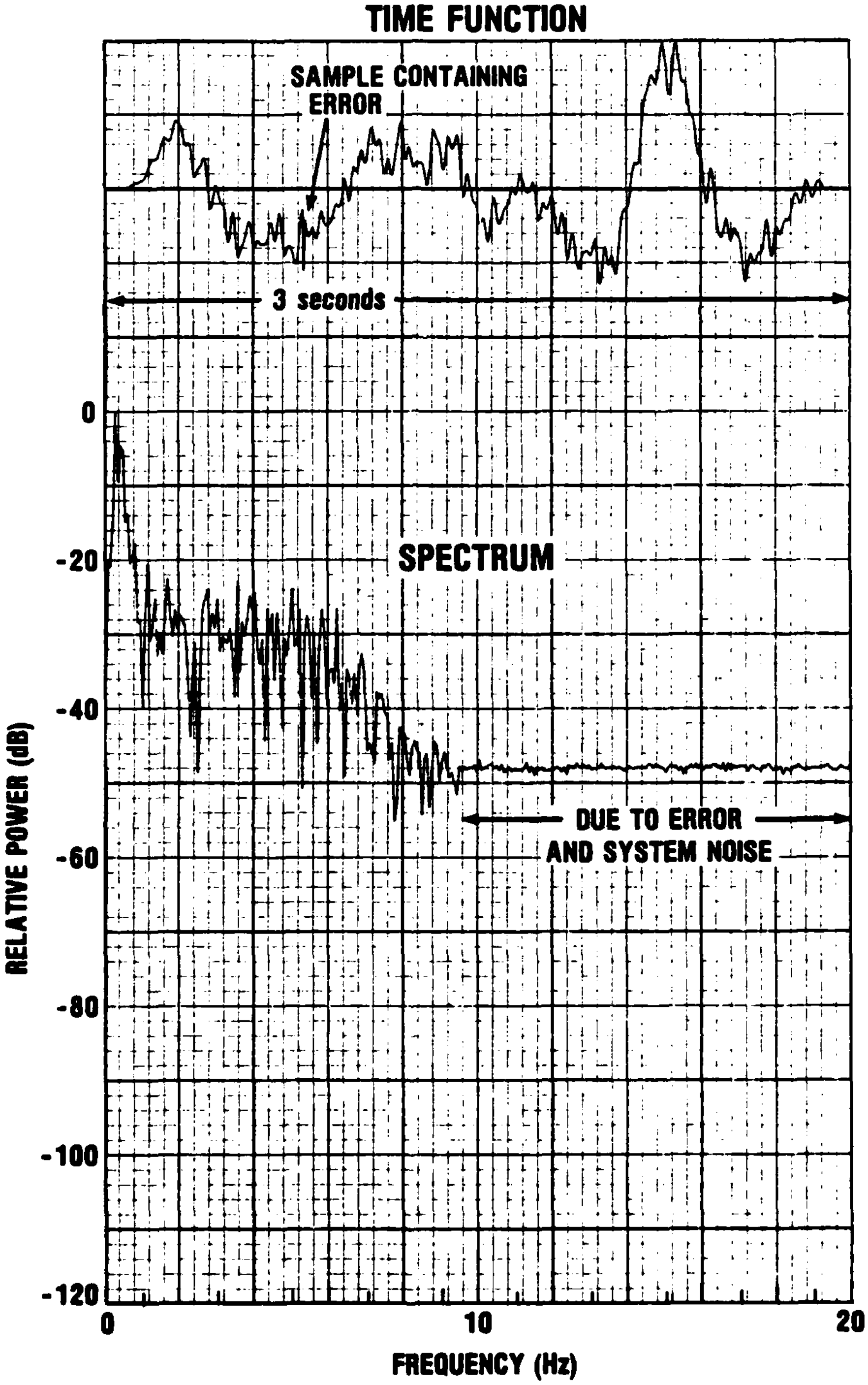
APPENDIX B

CORRECTION OF SINGLE BIT ERRORS IN NSS SHORT-PERIOD DATA

I. DESCRIPTION OF THE ALGORITHM

This appendix describes an algorithm that can correct most single bit errors in the NSS short-period data. The algorithm makes use of the fact that, although the short-period waveforms are sampled forty times per second, they contain little or no energy above 10 Hz. A single bit error in one of these channels is equivalent to the addition of an impulse to the error-free data, and the spectrum of this composite signal will contain energy in the 10 to 20 Hz region which is related primarily to the added impulse (see Fig. B-1). High-pass filtering can then be used to estimate the impulse, and this estimate, in turn, can be used to determine which bit of which data sample was in error.

In practice, the algorithm operates on a three-second interval of data. The first and last seconds of the interval are weighted with a raised cosine taper to eliminate edge effects, while the center one second has unity weighting. The complex spectra of the weighted data are computed with a Fast Fourier Transform, and the high-pass filter implemented by setting the Fourier coefficients for frequencies below 12 Hz to zero. The filtered spectrum is then inverse-transformed with an FFT to obtain a time domain representation of the high-pass filtered impulse. The time of the peak of this signal corresponds to the time of the sample containing the error, and its amplitude and sign, after suitable scaling, are equal to the amplitude and sign of the sample error introduced by the incorrectly received bit. This information, sample time and sample error, are then used in an attempt to correct the bit received in error.



10-22-81-12

FIGURE B-1. Time Function and Spectrum of NSS Short-Period Data Containing a Single Bit Error

This error correction attempt is not always successful. At times the impulse created by the bit error becomes lost in system noise. Figure B-2 illustrates this point. This figure shows the tapered time function and the corresponding high-passed version of this signal as artificial bit errors are introduced in the first through eighth bits of one sample. For errors introduced in bits one and two, the absolute peak of the high-passed signal does not occur at the time of the sample in error (indicated by the vertical lines on the figure), and modifications made on the basis of this peak would create an additional error. For errors in bits three through sixteen, however, the algorithm makes the desired correction.

In addition to the phenomenon noted above, the algorithm occasionally make incorrect decisions on which bit to correct if the error is in the gain-ranging bits (15 and 16) of the sample.

An empirical test of the algorithm was performed using 1,000 seconds of data collected at the prototype NSS station at McMinnville, Tennessee. This data set included both large and small earthquakes at regional and teleseismic ranges, ranges, several Soviet nuclear explosions, and periods of noise alone. The average probability of correcting a single bit error was 80 percent, and this performance was uncorrelated with the data in which the errors were introduced. That is, there was no more observable tendency toward failures of the algorithm for large or small signals than for noise. No correlation was observed between algorithm failures and data containing large seismic signal discontinuities (e.g., the onset of signals from a nuclear explosion).

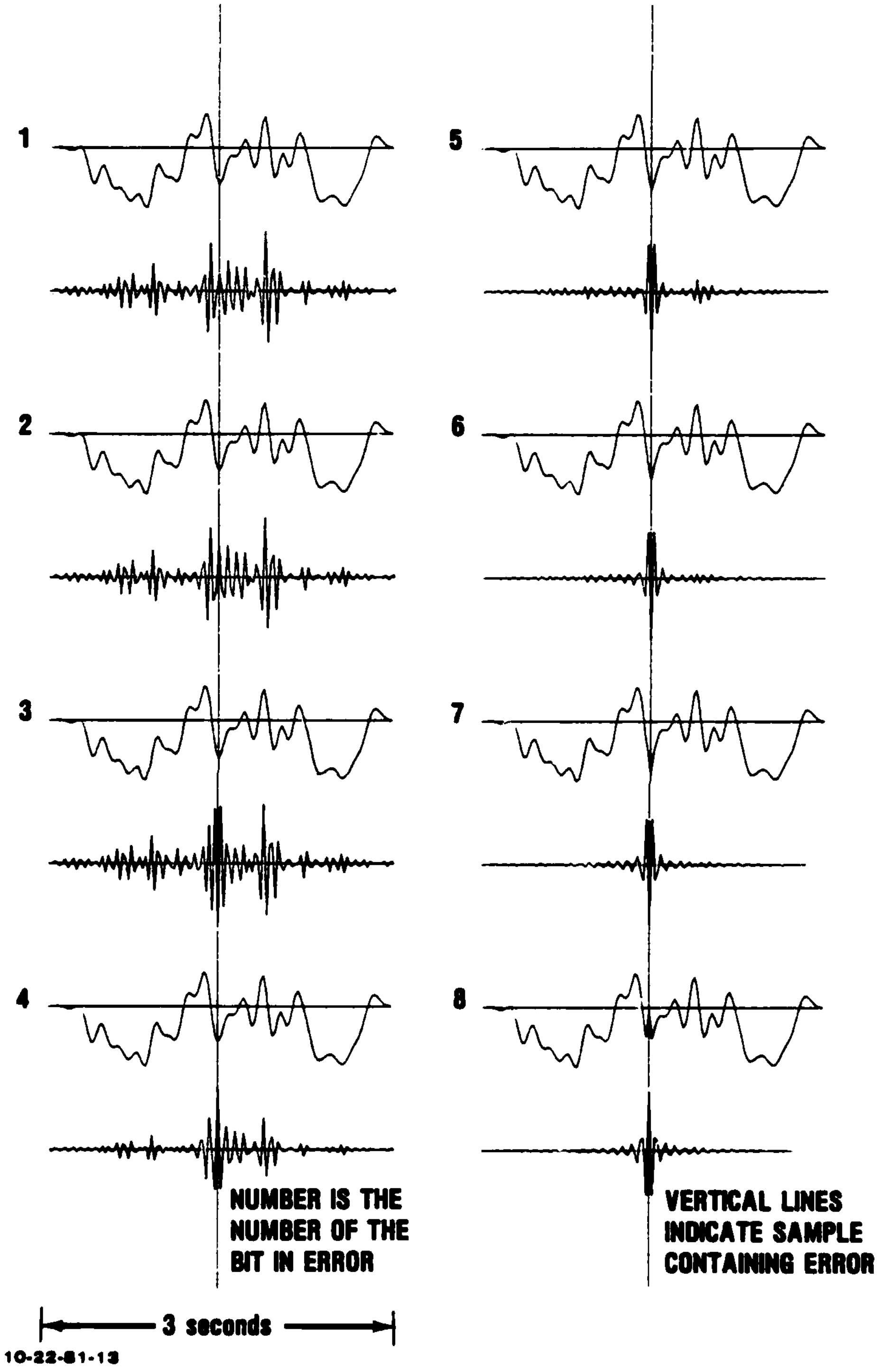


FIGURE B-2. Raw and Filtered Seismic Waveforms Containing Single Bit Errors

II. THEORETICAL PERFORMANCE PREDICTION

Because the short-period samples of seismic signals represent the bulk of NSS data transmitted to the SCARS, and also because the mean time between bits received in error is large (see III.A), the ability to correct 80 percent of the errors which occur in the short-period data should materially increase the mean time between authentication failures (MTBAF) for the system. This performance improvement will be independent of such other factors as forward error correction, redundant transmissions, or improved signal-to-noise ratio. To estimate the performance improvement possible, it is first necessary to restate the NSS data format in a form more readily suited for calculations.

Once the bits in an NSS data frame which are known à priori at SCARS* (e.g., synch preamble, ID/FA words, etc.) are substituted for the appropriate bits in the received frame, there will be 2256 received bits which may contain transmission induced errors. In addition to these bits, there will also be authentication bits which, if received in error, may cause the frame to fail authentication. If we assume no changes in the authentication algorithm (two ten-bit words), but require, as suggested in I.F.8, that we consider one authentication word 20 bits in length, we may restate the NSS data frame format as illustrated in Fig. B-3, which shows the frame as two separate date fields. The second of these data fields contains the short-period samples with 640 bits/channel. The first field contains the authentication word and a sub-field, all other, which includes the mid-period and long-period samples, state of health, etc.

*See Section III.B.2.

AUTH	ALL OTHER	SPZ	SPN	SPE
20	336	640	640	640
FIELD 1		FIELD 2		

2276 bits (1 second)

FIGURE B-3. Revised Description of the NSS Data Format

For a frame to authenticate, the first field must be error free, and the second field error free or contain only correctable errors. The probability that the first frame will be error free is:

$$P_1 = (1 - P)^{20+336} \simeq 1 - 356 P \qquad P \leq 10^{-5} \qquad (1)$$

where P is the probability that a bit is received in error. Because our ability to correct errors in one short-period channel does not depend on the remaining short-period channels (in fact, we can potentially correct single errors simultaneously in all three channels), we begin our discussion of the second field by considering only a single short-period channel. Since each short-period channel must be error-free, or contain only a single correctable error, the probability that a given short-period channel will contribute toward frame authentication, P_{SPCOK}, is

$$P_{SPCOK} = \underbrace{(1 - P)^{640}}_{\text{no error}} + \underbrace{640 P (1 - P)^{639}}_{\text{single error}} \times P_{PC} \times P_C \qquad (2)$$

where P_{PC} is the probability of being potentially correctable
P_C is thc probability of successful correction = 0.8.

An error in the data for one short-period channel of a given frame is potentially correctable only if the data for the same channel is error-free in both the frame preceeding and that following the frame containing the error. While this situation could exist even though either or both of these frames failed to authenticate because of errors in other portions of the frame, we would have no way of being certain of this fact. Thus, we will require that both the frames preceeding and following the frame containing the error authenticate. Noting that it represents a lower bound, the probability of an error being correctable will be given by:

$$P_{PC} \geq (1 - P)^{2276x2} \simeq 1 - 4552\ P\ . \qquad (3)$$

Rearranging and simplifying terms, we may rewrite Eq. 2 as

$$P_{SPCOK} \simeq 1 - 640\ P + 512\ P\ (1 - 639\ P)\ (1 - 4552\ P)$$

$$\simeq 1 - 128\ P \qquad P \leq 10^{-5}\ . \qquad (4)$$

Since all three short-period channels must meet the requirement stated in (4) for the frame to authenticate, the probability of the second field in the frame leading to authenticate will be:

$$P_2 = P^3_{SPCOK} \simeq 1 - 384\ P \qquad (5)$$

and the probability that the frame authenticates will be

$$P_A = P_1 P_2 \simeq 1 - 740\ P \qquad (6)$$

or the probability of authentication failures with only one transmission available at SCARS is

$$P_{FS} \simeq 740\ P\ . \qquad (7)$$

If two transmissions of each data frame are available at SCARS, we may make use of the second transmission to lower the probability of authentication failure. Let us first consider Field 1 of a date frame. Note that we can use the authentication bits of one transmission with the all other bits from the second transmission to obtain an error-free first field. Thus,

$$P_1 = \{1 - [1 - (1 - P)^{336}]^2\}\{1 - [1 - (1 - P)^{20}]^2\}$$
$$\simeq 1 - 1.133\ P^2 \times 10^5\ . \tag{8}$$

(U) For a single channel in the second field to cause a failure of authentication, it must contain an uncorrectable single bit error or a multiple bit error. Thus, P_{SPCNOK} will be

$$P_{SPCNOK} = 1 - P_{SPCOK} \tag{9}$$

and the probability that at least one of the two replicas of the data for this channel will be error-free or contain only a correctable error will be

$$P_{RSPCOK} = 1 - P^2_{SPCNOK} \simeq 1 - 128^2 P^2\ . \tag{10}$$

Since all three short-period channels must meet the requirement of Eq. 10, the probability that the second field will contribute to authentication is

$$P_2 = P^3_{RSPCOK} \simeq 1 - 49{,}152\ P^2 \tag{11}$$

and the probability of authentication is

$$P_A = P_1 P_2 \simeq (1 - 113{,}300\ P^2)(1 - 49{,}152\ P^2)$$
$$\simeq 1 - 162{,}452\ P^2 \tag{12}$$

and the probability of a frame not authenticating when both transmissions are available at SCARS is

$$P_{FR} \simeq 162{,}452 \; P^2 \; . \qquad (13)$$

Using the probability of authentication failure given in Eq. 7, the MTBAF for NSS transmissions without redundancy (the 15-minute delayed transmission is ignored) but using the short-period, error-correcting algorithm will be:

$$\text{MTBAF (single transmission)} \simeq P_{FS}^{-1} \simeq \frac{1}{740 \; P} \text{ seconds} \; . \qquad (14)$$

When both the direct and 15-minute delay transmissions are both used, we must take into account the satellite link outages of less than 15 minutes duration to calculate an MTBAF for the system. From Appendix C, the number of frames per year for which only a single transmission is available at SCARS, NSDL, is

$$\text{NSDL} \simeq 5{,}477 \text{ n frames} \qquad (15)$$

and the number of frames per year that both transmissions are available, NRDL, is

$$\text{NRDL} \simeq 31{,}536{,}000 - 34{,}970 \text{ n frames} \qquad (16)$$

where n is the number of ground terminals in the link. For our hypothesized three-satellite link (see Fig. 10), there are four ground terminals susceptible to failure; two each at the relay points in Japan and the U.S. west coast. Thus, NSDL and NRDL become:

$$\text{NSDL} \simeq 21{,}908 \text{ frames}$$
$$\text{NRDL} \simeq 31{,}396{,}120 \text{ frames.}$$

The expected number of uncorrected errors per year for the time that both transmissions are available at SCARS will be

$$\hat{N}_R \simeq \text{NRDL} \times P_{FR} \simeq 5.10\ P^2 \times 10^{12} \qquad (17)$$

and the expected number of uncorrected errors per year when only a single transmission is available at SCARS will be

$$\hat{N}_S \simeq \text{NSDL} \times P_{FS} \simeq 1.62 \times 10^7\ . \qquad (18)$$

The total expected number of uncorrected errors per year is simply the sum of N_S and N_R, and the MTBAF for the redundant transmission case will be:

$$\text{MTBAF}_{\text{redundant}} = \frac{1}{\hat{N}_S + \hat{N}_R} \text{ years}$$

$$\simeq (1.62\ P \times 10^7 + 5.10\ P^2 \times 10^{12})^{-1}\ . \qquad (19)$$

Before leaving this topic, let us evaluate the MTBAF for the prototype NSS. Recall that the link budget for the prototype (see Ref. 3) provided for a probability of a bit error of 10^{-7} for a single satellite link. Then, with a three-satellite link, $P = 3 \times 10^{-7}$ (see Section III.A), and

$$\text{MTBAF (Single)} \simeq 1.25 \text{ hours}$$

and

$$\text{MTBAF (Redundant)} \simeq 0.188 \text{ years}\ .$$

It should also be noted that there will be an average of 32.8 hours/years when there will be no satellite data available for this three-hop link (see Appendix C).

APPENDIX C

THE EFFECT OF SATELLITE LINK OUTAGES ON REDUNDANCY FOR NSS/SCARS COMMUNICATIONS

APPENDIX C

THE EFFECT OF SATELLITE LINK OUTAGES ON REDUNDANCY FOR NSS/SCARS COMMUNICATIONS

During the design phase for the prototype NSS, it was recognized that there would inevitably be a number of periods during each year when the satellite links between the NSS remote stations and the SCARS would be broken. Two design features were incorporated to make certain that sensor output data gathered during these periods would not be lost. For long circuit outages, a tape recorder was provided to save the data, and for short circuit outages, a digital delay line was included so that both real-time and delayed data streams would be available for transmission to the SCARS. It should be noted that, for outages shorter than the delay time, SCARS would receive the sensor outputs in sufficient time to make effective use of other national technical systems, a situation not true for the longer outages which would require physical transmission of the tape recordings to the SCARS. Considering both bubble memory technology and reported INTELSAT availability statistics at the time of the NSS prototype design, a 15-minute length was chosen for the digital delay line.

The result of this choice is that most of the time both real-time and delayed data are available at the SCARS. Some fraction of the time only a single transmission of data is available (either the real-time or 15-minute late data), and for another fraction of time, no data is available at SCARS until the tape recordings are collected at the field sites and shipped to the U.S., a process which is estimated to take at least one month. For this study, we will not consider the intervals for which the recorder is used, but will concentrate on those periods for which single or redundant satellite transmissions of data are available at the SCARS, since a knowledge of the times that single or redundant data are available is necessary to compute the MTBAF for the NSS.

Let us begin by noting that outages in satellite links are primarily the result of ground station failures (Ref. 8), and we will ignore the contribution toward link outages contributed by failures in the space segments of these links. With this proviso, we reviewed the INTELSAT availability statistics* for 1978. These statistics showed an average of 43 outages/station/year. Of these outages, 11.82 percent lasted 15 minutes or more and will not be considered here since no satellite data would be available at SCARS during these outages. We are left then with an average of 37.9 outages (T < 15 min)/station/year which must be considered. Using the distribution of station outages by duration provided by INTELSAT, one can develop the probability density function given below:

INTERVAL (sec)	MEAN (sec)	PROBABILITY
$t < 2$	1	0.1810
$2 \leq t < 5$	2.5	0.0683
$5 \leq t < 10$	7.5	0.0728
$10 \leq t < 60$	35	0.2427
$60 \leq t < 120$	90	0.0939
$120 \leq t < 180$	150	0.0692
$180 \leq t < 240$	210	0.0543
$240 \leq t < 300$	270	0.0354
$300 \leq t < 600$	450	0.1384
$600 \leq t < 900$	750	0.0440

*It should be noted that the INTELSAT statistics include many poorly maintained third-world stations. Thus, the numbers arrived at in this appendix should be considered as lower bounds on performance of those ground stations which would actually be used with the NSS.

From this density function we find that the average duration/outage/station/year, T_{AVG}, is:

$$T_{AVG} = 144.46 \text{ seconds} .$$

Then, since there are an average of 37.9 outages/station/year ($T < 15$ min), the total average seconds of outage/station/year, or the duration of single data availability for a one-hop system,

$$T_{SDIH} = 37.9\ T_{AVG} = 5{,}475 \text{ seconds.}$$

To find the number of seconds when redundant data is available with a one-hop system, we must take into account that the average time of outage/station/year (all duration outages) is 34,970 seconds. Thus, there are 34,970 - 5,475 = 29,495 seconds which are recorded, and the average time/station/year when redundant data is available is:

$$\begin{aligned} T_{RDIH} &= 31{,}536{,}000 \text{ (seconds/year)} - 29{,}495 \text{ (seconds} \\ &\quad \text{with no satellite data)} - 5{,}475 \text{ (seconds with} \\ &\quad \text{only single data available)} \\ &= 31{,}501{,}030 \text{ seconds.} \end{aligned}$$

Let us now extend our calculations to the multihop satellite circuit. Here we assume that the ground station outages are independent. Next we note that the total outage time/station is a small percentage of the total time, approximately 0.1 percent. We will then approximate the total seconds of outage/link (n ground terminals/link)/year with only single data available as:

$$T_{SDL} = 5{,}475\ n \text{ seconds}$$

and the total seconds/link/year with redundant data available is approximated as

$$T_{RDL} = 31,536,000 - 34,970 \text{ n seconds.}$$

Finally, it should be noted that there will be approximately 29,495 n seconds or 8.2 n hours/link/year during which no satellite data will be available.

APPENDIX D

REDUNDANT GROUND STATIONS FOR THE NSS SATELLITE DATA LINK

APPENDIX D

REDUNDANT GROUND STATIONS FOR THE NSS SATELLITE DATA LINK

This appendix discusses the use of redundant ground stations to minimize the time for which no satellite link data is available to the SCARS. We make three assumptions for the following discussion. First, failures of the NSS remote ground stations need not be considered since without these stations there will be no data to authenticate. Second, the SCARS receiver possesses sufficient redundancy that failures of this terminal can be ignored. Third, the domestic satellite availability statistics are as good as those experienced by INTELSAT,* and can be ignored.

A suggested architecture for redundant ground stations for an NSS satellite link is shown in Fig. D-1. Signals leaving the Indian Ocean Satellite proceed to the SCARS by two paths, A and B, each of which pass through four ground stations susceptible of failure. Using the 1978 INTELSAT availability statistics, we expect an average of 42.96 outages/ground station/year with an average duration/outage of 13.57 minutes. Since the average duration of these outages is very small compared to the mean time between outages (13.57 << 525,600), and since hardware failures are independent from station to station, we may approximate the average annual number of failures for each link by the product of the average number of outages/station/year and the number of ground stations. Thus,

$$\bar{N} \simeq 4 \times 42.96 \simeq 171.84 \text{ per year },$$

*No failures of the space segment for the last two years (Ref. 8).

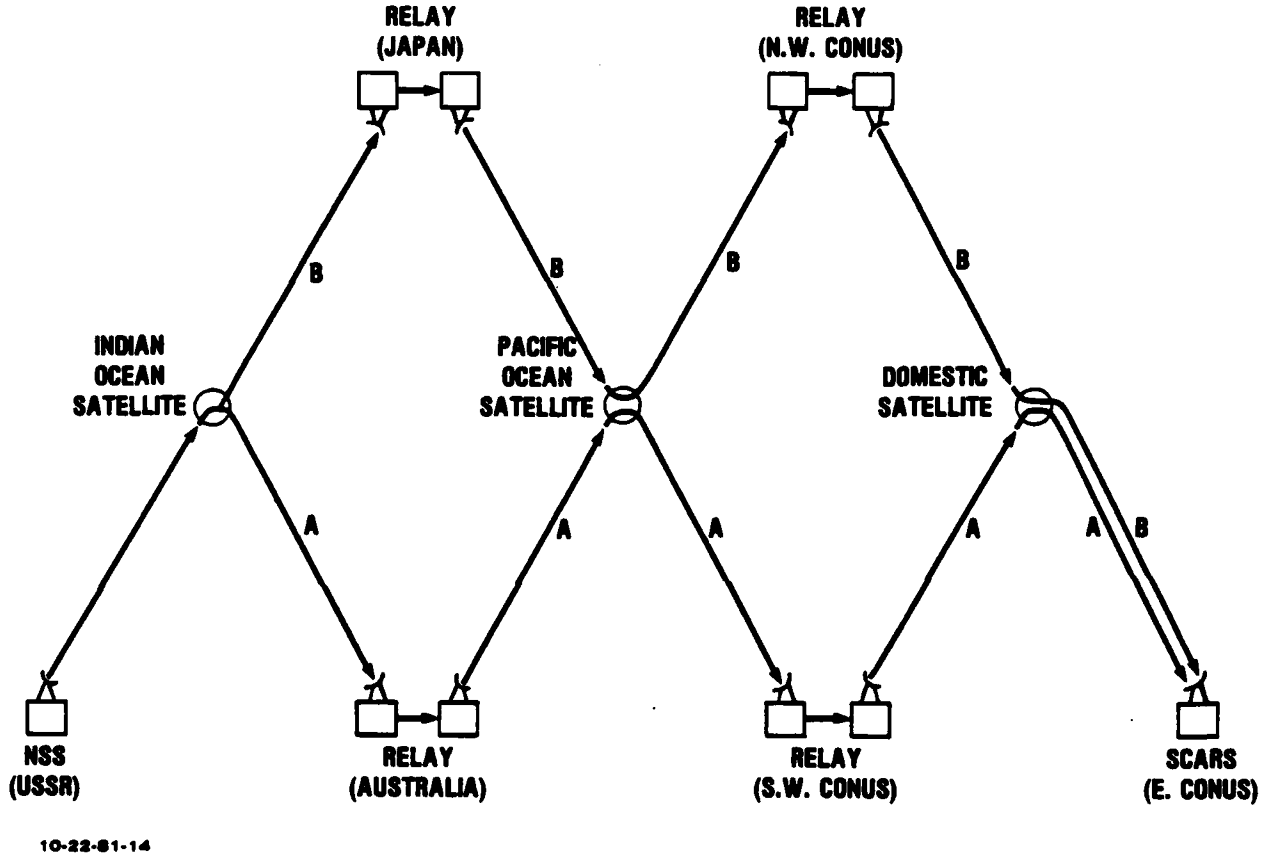


FIGURE D-1. NSS Data Link with Redundant Earth Stations and the availability for a given path will be

$$A_P \simeq [525{,}600\ (\text{min/yr}) - \bar{N} \times 13.57]/525{,}600 \simeq 0.9956. \quad (1)$$

We take the probability of a path failure to be

$$P_{PF} \simeq 1 - A_P \quad (2)$$

For a single path, there will be an annual average outage of 38.9 hours. For two paths in parallel as shown in Fig. D-1, the expected time for which there will be no connectivity between the remote station and SCARS (simultaneous failure of both paths) will be

$$T_{ND} \simeq P_{PF}^2 \times 31{,}536{,}000 \simeq 620.8\ (\text{seconds/year}); \quad (3)$$

the expected time for only one path available will be

$$\hat{T}_{1P} \simeq 2\ P_{PF}\ (1 - P_{PF}) \times 31{,}536{,}000 \simeq 278{,}598\ (\text{seconds/year}); \quad (4)$$

and, the expected time with both paths available will be

$$\hat{T}_{2P} \simeq (1 - P_{PF}^2) \times 31{,}536{,}000 \simeq 31{,}535{,}379\ (\text{seconds/year}). \quad (5)$$

END

FILMED